AF/ 2143 $

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Foncarnier**

Serial No.: **09/407,738**

Filed: **September 28, 1999**

For: **Method and System for Broadcasting Alarm Messages to Selected Users of an IP Network**

Group Art Unit: **2143**

Examiner: **Jaroenchonwanit, Bunjob**

Attorney Docket No.: **FR9-98-059**

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Mailing Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 25, 2004.

By: Rebecca Clayton
Rebecca Clayton

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appellant's Brief (in triplicate) (37 C.F.R. 1.192); and
- Our return postcard.

A fee of $330.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANT

Docket No. FR9-98-059 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Foncarnier** §

§ Group Art Unit: **2143**

Serial No. **09/407,738** §

§ Examiner: **Jaroenchonwanit, Bunjob**

Filed: **September 28, 1999** §

§

For: **Method and System for Broadcasting Alarm Messages to Selected Users of an IP Network** §

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

Certificate of Mailing Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 25, 2004.

By: Rebecca Clayton
Rebecca Clayton

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on April 29, 2004.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

REAL PARTIES IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines, Inc.

RELATED APPEALS AND INTERFEERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-24

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-24
4. Claims allowed: NONE
5. Claims rejected: 1-24

C. CLAIMS ON APPEAL

The claims on appeal are: 1-24

STATUS OF AMENDMENTS

No amendments to the claims after mailing of the Final Office Action have been made.

SUMMARY OF INVENTION

The present invention is directed to a system, method and computer program product for broadcasting alarm messages to selected users in a heterogeneous data transmission network such as an Internet Protocol network. The alarm messages are broadcast to a list of users defined by their profiles which have been previously stored in a profile table. The system includes a profile table which contains the profiles of each user and a processing and transmitting means which enables an administrator associated with the server to transmit alarm messages to the list of users. The users in the list of users are selected by selecting profiles in the profile table. The alarm messages may be manually written and sent by the administrator when necessary.

ISSUES

The issues on appeal are as follows:

(1) whether or not the objection to the drawings as allegedly not showing a selecting means or step of selecting a list of users as recited in claims 22-24 is proper;

(2) whether or not the objection to the specification under 35 U.S.C. § 112, first paragraph as allegedly failing to disclose that a list of users is a subset of the plurality of users is proper;

(3) whether or not the rejection of claims 22-24 under 35 U.S.C. § 112, first paragraph as containing features that are allegedly not described in the specification is proper;

(4) whether claims 1, 8, and 15 are obvious under 35 U.S.C. § 103(a) over Stupek, Jr. et al. (U.S. Patent No. 6,131,118);

(5) whether claims 2-5, 7, 9-12, 14, 16-19, and 21 are obvious under 35 U.S.C. § 103(a) over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) in view of Drala Software, "Event Notifier, a Pattern for Event Notification," published in Java Report, July 1998, Volume 3, Number 7;

(6) whether claims 6, 13, and 20 are obvious under 35 U.S.C. § 103(a) over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) and in further view of Drala software, "Event Notifier, a Pattern for Event Notification," published in Java Report, July 1998, Volume 3, Number 7 and further in view of Cote et al. (U.S. Patent No. 6,021,262);

(7) whether the rejections of claims 22-24 under 35 U.S.C. §102(e) based on Raffel et al. (U.S. Patent Publication 2002/0082892) and Ruckdashel et al. (U.S. Patent No. 6,038,542) are proper;

(8) whether claims 22-24 are anticipated by Raffel et al. (U.S. Patent Publication 2002/0082892) under 35 U.S.C. § 102(e); and

(9) whether claims 22-24 are anticipated by Ruckdashel et al. (U.S. Patent No. 6,038,542) under 35 U.S.C. § 102(e).

GROUPING OF CLAIMS

The claims do not stand or fall together but instead stand or fall in accordance with the following grouping of claims, reasons for such groupings being provided in the following arguments:

Group I:	claims 1, 2, 7, 8, 9, 14, 15, 16 and 21
Group II:	claims 3, 10, and 17;
Group III:	claims 4, 11, and 18;
Group IV:	claims 5, 12, and 19;
Group V;	claims 6, 13 and 20; and
Group VI:	claims 22-24.

ARGUMENT

I. Objection to the Drawings

The Final Office Action objects to the drawings under 37 CFR 1.83(a) because they allegedly do not show the feature of the selecting means and the step for selecting a list of users as recited in claims 22-24. Appellant respectfully submits that support for these features is provided at least in Figure 1 of the present invention. Specifically, Figure 1 contains an Administrator Interface 22, a Profile Table 24 and a Processing Unit 20, all of which contributes to a means for selecting a list of users based on profile information in the profile table and performs the steps of selecting users from the Profile Table 24.

Page 4, lines 7-14 of the present specification discloses the relationship between the Administrator Interface 22 and the Profile Table 24 in selecting a list of users based on profile information in the profile table:

> A message or an alarm can be manually sent when the server administrator writes the message (or alarm) on Administrator Interface 22 and initiates the transmission thereof to a list of users whose profile has been selected in Profile Table 24. Then, the message is sent by Message Sender 28 over the network to all running workstations corresponding to the selected profile. On the user workstation, the Java alarm program receives the message (or alarm) and displays it on the foreground of the user screen, and an alarm tune is also played. Once the message is read, the user presses the OK key and the program switches in the background. Then, the Java alarm program sends back to server 16 an acknowledgement which can be used for statistic purposes on the server.

In addition, page 3, lines 16-21 describe the administrator interaction with Processing Unit 20 in selecting a list of users based on profile information in the profile table:

> Server 16 includes a Processing Unit 20 which handles the server and is also used to process all the operations controlled by an administrator entering the server via an administrator interface 22. Server 16 also comprises a System Network Messaging Protocol (SNMP) Interface 23 to monitor defined machines, a Profile Table 24 for the registration of user profiles, an Alarm Scheduler 26 and a Message Sender 28 connected to node 18.

Thus, the present specification clearly states that the administrator interacts with server 16 using Administrator Interface 22. The Administrator selects users through Administrator Interface 22 from Profile Table 24. In addition, it is clear from Figure 1 and the sections

reproduced above that the Processing Unit 20 allows an interaction between the Administrator Interface 22 and the Profile Table 24. Thus, the means for selecting a user resides in the Administrator Interface 22, the Processing Unit 20, or a combination of the Administrator Interface 22 and the Processing Unit 20.

Thus, despite allegations made in the Office Action, Figure 1 does, in fact, depict the feature of the selecting means and the step for selecting a list of users as recited in claims 22-24. Therefore, the objection to the drawings under 37 CFR 1.83(a) is overcome.

II. 35 U.S.C. § 112, First Paragraph

The Final Office Action objects to the specification under 35 U.S.C. § 112, first paragraph, as failing to adequately teach how to make and/or use the invention in claims 22-24. Additionally, the Office Action rejects claims 22-24 under 35 U.S.C. § 112, first paragraph, for the same reasons. This objection and rejection are respectfully traversed.

In rejecting claims 22-24 under 35 U.S.C. § 112, first paragraph, the Office Action states:

> The specification is objected to under 35 U.S.C. § 112, first paragraph, as failing to adequately teach how to make/or use the invention, i.e., failing to disclose list of user is a subset of the plurality of users. Appellant's disclosure is insufficient to allow one of ordinary skill in the art to make or use the invention without undue experimentation because Appellant did not adequately disclose the necessary apparatus to perform the claimed method. See In re Gunn, 190 USPQ 402, 406 (CCPA 1976). In fact Appellant's disclosure did not even sufficiently include selecting means and method step of selecting a list of users, which is a subset of the plurality of user, based on profile information in the profile table on which the claimed method and system could be implemented.

Office Action dated January 29, 2004, page 2.

Appellant respectfully disagrees and directs the Board's attention to page 3, lines 1-8 of the present specification, which reads as follows:

> Therefore, the invention relates to a system for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using the Java language. This system comprises a profile table which contains the profiles of each user, and processing and transmitting means which enable an administrator associated with the server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table, the alarm messages being displayed on the screen of

the workstation associated with each selected user if the workstation is running.

Thus, the present specification states that the alarm message is sent to a list of users among a plurality of multi-platform users. In other words, the plurality of multi-platform users is a set of users which contains a list of users as a subset of the plurality of multi-platform users. The list of users selected from the profile table is among the plurality of multi-platform users. Thus, the present specification discloses that the list of users is a subset of the plurality of users.

In addition, as set forth above, Figure 1 of the present application discloses the selecting means and method for selecting a list of users. Thus, the present specification does, in fact, disclose that the list of users is a subset of the plurality of users. Similarly, the present specification also discloses a selecting means and method of selecting a list of users, which is a subset of the plurality of users, based on profile information in the profile table. Therefore, the objection of the specification and the rejection of claims 22-24 under 35 U.S.C. § 112, first paragraph has been overcome.

III. 35 U.S.C. § 103, Alleged Obviousness of claims 1, 8, and 15

The Final Office Action rejects claims 1, 8, and 15 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118). This rejection is respectfully traversed.

With regard to claims 1, 8 and 15, the Office Action states:

> As to claims 1, 8, and 15, Stupek a flexible display of management data in programmable event driven processing system, the system comprises a server for detecting and receiving an event from network devices and transmits the event notification to the user based on the event defined in database, the system comprising
>
> profiling in a profile table each one of said plurality of users (Stupek teaches, a network management server, which included a database that containing user preferences, enabled the user to specify specific event monitoring, Col. 5, lines 46-67, database and user preference is considered equivalent to profile table);
>
> transmitting said alarm message to the list of users wherein said users have been selected from said profile table, said alarm message being displayed on a screen of a workstation associated with each selected user if said workstation is on (Stupek teaches, the management server enabled the user to select and view various information including the selected events, Col. 6, lines 7-15. Inherently,

Stupek also teaches transmitting the alarm or event messages from the management server to user terminal).

Stupek does not explicitly disclose an administrator is associated with the server.

Official Notice is taken (see MPEP 2144.03) that administrator processed alarm was well known in the network management system.

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to associated network administrator with Stupek network management server to process alarm of event notification event. Doing so, the management capabilities, flexibility would be enhanced, because the system can be intervened by a human, which would allow the system to be configured to accommodate with most if not all situations.

First Office Action dated September 17, 2003, pages 2-3.

Claim 1, which is representative of claims 8 and 15 with regard to similarly recited subject matter, reads as follows:

1. System for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using Java language, said system being characterized in that it comprises:

a profile table containing profiles of each one of said plurality of users; and

processing and transmitting means enabling an administrator associated with said server to transmit alarm messages to the list of users wherein said users have been selected from said profile table, said alarm messages being displayed on a screen of a workstation associated with each selected user if said workstation is running. (emphasis added)

Stupek, Jr. (Stupek hereafter) is directed to a network management system that facilitates and performs programmable event driven processing including event detection logic that receives and processes any of a plurality of event notifications transmitted via the network. The network management server and the managed devices can be accessed remotely from a client system via an intranet or the Internet using a web browser. The client, if authorized, can access and view the management information regarding the managed devices. The client sends an HTTP request to a network management server or a managed device for a web page which is then passed back to the client system. Once the client logs onto the webpage, management information can be monitored

from the client device and the client can perform administrative duties (column 1, lines 55-60 and 63-67 and column 6, lines 15-30).

Thus, Stupek is concerned with performing network management functions, much like the Simple Network Management protocol (SNMP) and the Desktop Management Interface (DMI), across the Internet using a web browser. Although Stupek may allow for the client to define certain preferences and identify certain data to be monitored, there is nothing in Stupek that teaches or even suggests an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table as recited in claims 1, 8, and 15 of the present invention. The Final Office Action alleges this feature is taught in the following section of Stupek:

> The management server **102** enables the user to select a managed element **104** and view detailed information about that device. The management server **102** also enables a user to create device groups for business process views by filtering for selected devices and for selected events of those devices. The management server **102** handles events, such as SNMP traps and HTTP alerts, logs the events, and allows a user to set event filters.
>
> (column 6, lines 7-14)

This section merely describes the interaction between the user (administrator) and the management server. The user may view device information or set user specified monitoring preferences, enabled by the management server. Nowhere in this section or any other section of Stupek is it taught or suggested to transmit alarm messages to a list of users, selected from a plurality of users within a profile table as recited in claims 1, 8, and 15 of the present invention.

Furthermore, the Office Action states, "Inherently, Stupek also teaches transmitting an alarm or event message from the management server to user terminal" (see First Office Action, page 3). While a transfer of data in Stupek may occur from the management server to the user terminal, the data transfer is not in response to a list of users being selected from a plurality of users within a profile table, as recited in claims 1, 8, and 15 of the present application. Rather the information is transferred from the management server to the user terminal in response to a request for information made by the user.

In addition, Appellant agrees with the Examiner that Stupek does not teach that an administrator is associated with the server. The Final Office Action, however, alleges this feature is old and well known. While an administrator being associated with a server may be old and well known, the present invention does not simply claim that an administrator is associated with the server. Rather the present invention recites having an administrator associated with the server transmit alarm messages to a list of users wherein the users have been selected from a profile table.

Furthermore, this is not the problem that Stupek is concerned with and thus, Stupek does not even hint at an administrator associated with the server transmitting alarm messages to a list of users that have been selected from a profile table. To the contrary, Stupek is merely concerned with processing event notifications and does not discuss the sending of alert messages by an administrator to users selected from a profile table. Therefore, Appellant respectfully submits that Stupek does not teach or suggest the features of independent claims 1, 8, and 15.

Examiner's Response to Appellant's Arguments

With regard to the above arguments, the Final Office Action states:

> Appellant's arguments filed on 12/17/2003 have been fully considered but they are not persuasive. In the remarks, Appellant argued in substance that:
>
> (a) Prior art failed to teach administrator associated with a server sending alarm to a list of user, selected from a plurality of users within a profile table, as recited in claims 1, 8 and 15.
>
> As to point (a), Examiner disagreed, there is no support in neither specification nor claims that suggested a list of user is or must be selected from users within a profile table. Without specific support, the examiner can interpret the claims' language as, selecting user(s) based on his or her profiles and sending a notification to the user(s) whose profile meet a criterion. Further, the examiner noted that the claims language read on many event notification systems, e.g., contact list notification, news or services subscribing, which sent the notification on users registration, subscriptions or users profiles basis. Since, there is no specific profile structure was taught in the disclosure. The examiner, therefore, allowed to give the broadest reasonable interpretation to such claims' limitation. Furthermore, nowhere in the disclosure that suggested a list of users, i.e., user names, must be within the profile table, thus, a database contains objects' profile could be construed as a profile table. It is not necessarily that the profile table must contain list of users' name, it could be a plurality of object's profiles, which

are associated with a plurality of users. Selectively, bases on a criterion, the system could form a list of users from the profiles that met the criterion, for receiving the notification(s). And, that was taught in Stupek, the interconnection engine relays a particular event based on registration information, (Col. 9, lines 1-46); in one embodiment it includes action category that includes threshold tools allow the user to be notified whenever the certain condition arise, (Col. 7, lines 10-64).

Thus, the Examiner states in the Final Office Action that there is no support in either the specification or the claims that suggests that a list of users is, or must be, selected from users within a profile table and that because of this alleged lack of support, the Examiner may interpret the claims in any manner he sees fit, such as interpreting the claims to allegedly read on the cited prior art. Appellant respectfully disagrees and directs the Board's attention to the language of originally filed claim 1. Specifically, claim 1 recites a profile table containing profiles of each one of a plurality of users and processing and transmitting means enabling an administrator associated with said server to transmit alarm messages to a list of users wherein the users have been selected from the profile table. Thus, the profile table contains profiles for a plurality of users and alarm messages are sent to users selected from the plurality of users within the profile table. These selected users constitute the list of users to which the alarm messages are transmitted. Thus, claim 1 itself supports the position that the list of users is selected from a plurality of users represented in the profile table.

Additionally, the present specification also provides support that the list of users is selected from users in a profile table, for example, at page 2, line 17 – page 3, line 8, which reads as follows:

> Another object of the invention is to provide a heterogeneous data transmission network such as an IP network wherein at least a server can broadcast information and alarm messages to a list of users defined by their profiles previously stored in a profile table
>
> Therefore, the invention relates to a system for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using the Java language. This system comprises a profile table which contains the profiles of each user, and processing and transmitting means which enable an administrator associated with the server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table, the alarm messages being displayed on the screen of the work station associated with each selected user if the workstation is running.

(emphasis added)

Further support for this feature is also provided at page 3, lines 1-8, which is reproduced above. This section clearly recites the feature of enabling an administrator associated with a server to transmit alarm messages to the users of the list wherein the users have been selected by selecting profiles in the profile table. Additional support can also be found at page 4, lines 7-9, which is also reproduced above. This section states that "a message or an alarm can be manually sent when the server administrator writes the message (or alarm) on Administrator Interface 22 and initiates the transmission thereof to a list of users whose profile has been selected in Profile Table 24."

Thus, the present specification specifically recites the feature of a profile table containing profiles of a plurality of users. Additionally, the present specification also recites the feature of selecting a list of users by selecting profiles in the profile table. Thus despite allegations made by the Examiner in the Final Office Action, both the claim language and the present specification provide support for a list of users being selected from users within a profile table. Therefore, the Examiner cannot simply disregard what is actually recited in the claims and come up with his own unsupported interpretation of the claim language just so it appears as though the claims read on the cited art.

In addition, the Examiner states that the present specification does not specifically recite that the profile table must contain a list of users' names. Therefore, the Examiner interprets the profile table as containing a plurality of object profiles, which are associated with each of a plurality of users, wherein the system could form a list of users from profiles that meet certain criterion for receiving notifications.

First, this argument is extraneous to the actual claim language. Nowhere in the claims is there any recitation of "users' names" and thus, the Examiner's arguments with regard to this topic are irrelevant. Second, even if the Examiner chooses to interpret the profile table in such a manner, Stupek still does not teach that a profile table contains a plurality of object profiles, which are associated with each of a plurality of users, wherein the system may form a list of users from profiles that meet certain criterion for receiving notifications, despite allegations made in the Final Office Action.

In Stupek, the event must meet certain criteria in order for a notification to be sent to the administrator. In the claimed invention, the users, or user profiles, must meet certain criteria in order to receive a notification. There is simply nothing in Stupek that teaches a list of users is selected based on a profile to receive an alarm message, let alone an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table as recited in independent claims 1, 8 and 15. The Examiner, however, alleges that this feature is taught by Stupek at column 9, lines 1-46, which reads as follows:

> FIG. 3 is a block diagram of the AE 210 including the interconnect engine 212 that is responsible for connecting together events with constructions or "listeners" 302 of the events. In the embodiment of FIG. 3, the interconnect engine 212 receives an event signal or notification, either externally or from a construction 302, and relays the event to the appropriate one of the constructions 302. The interconnect engine 212 determines which construction 302 to relay the particular event to based on registration information that has been recorded in the interconnect engine 212. The interconnect engine 212 includes event detection logic for registering to receive events using interconnection logic and also passes those events to the proper constructions based on the registration information. Further, the event detection logic includes a server interface for interfacing with the network and a server event handler, coupled to the server interface and the interconnection logic, that routes event notifications received by the server interface to the interconnection logic. Thus, an event cycle is supported in which the interconnect engine 212 receives an event (either externally or internally) and then determines which destination construction(s) to send the event. Next, the construction(s) may generate an internal event and the internal event is passed back to the interconnect engine 212 to begin a new cycle. This cycle is repeated as necessary for the particular management operations of the system. The SNEH 226 registers as an event forwarder and receives events for which no listener has registered.
>
> Such unregistered events include net events received and transmitted via the HTTP server 224.
>
> FIG. 4 is a simplified block diagram of an exemplary construction 400 according to the present invention. The construction 400 of FIG. 4 includes, but is not limited to, one or more executable components 401, interconnection data structures 402, an executable component dispatcher 403, an event receiver (or event listener proxy) 404, and executable component statistics 405. The executable components 401 enable the construction 400 to be activated by notifying the event receiver 404 of the event parameters to monitor. One or more of the executable components 401 includes an event listener component to register with the event receiver 404 and becomes a listener for one or more specific events. The event receiver 404 serves as an event proxy for the executable components 401 by registering with the interconnect engine 212 to become a

listener of the one or more specific events.

This section has nothing to do with an administrator sending alarm messages to a list of users, selected from a plurality of users within a profile table. This particular section is directed to relaying events to the appropriate one of the constructions. The constructions are software components which contain one or more executable components, interconnection data structures, an executable component dispatcher, an event receiver (or event listener proxy), and executable component statistics. The executable components within the construction contain event "listeners". The term "listener" as used in Stupek refers to a mechanism for event detection. There is nothing in this section or any other section of Stupek that teaches or suggests an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table.

Further, the Examiner states that Stupek, at column 7, lines 10-64, teaches threshold tools that allow a user to be notified whenever certain conditions arise. This section, as well as surrounding text, reads as follows:

> There are many categories of actions that the management server 102 discovers. One action category is hardware fault detection, which is a category of actions identifying problems with hardware. Examples of hardware fault detection include failures or predictive failures on hard drives, processors, and memory. Most problem resolutions in the is hardware fault detection category are simply identified steps that the user must follow to correct the problem. Tools in this category allow viewing of the problem. Another action is software configuration actions, which are actions that identify potential problems with software configurations. Software configuration actions use version control functionality along with the concept of a "software set". The user establishes a set of software that should be loaded on a server, and this category of actions identifies any deviations from that set, and differences between the set and the latest software. Problem resolution for software configuration allows distribution of software updates, along with retrieval of new software. Tools in this category include software distribution, Internet download, and report generation.
>
> Another action category is thresholds, which are actions that track situations on the network identified by combinations of data. The user has to configure the situations. The threshold tools allow the user to monitor management data and be notified whenever certain conditions arise. Another action category is action advisories, which are actions that notify the user whenever an event is needed to be performed, such as service advisories generated by the manufacturer of the management server 102. Other advisory examples

include backups, disk storage cleanup, etc. Tools for this category provide the details of the action advisory and may allow corrective action. Another action category is software updates, which are actions that notify the user whenever a new software update to software on their network becomes available on a corresponding web site. Tools for this category allow the new update to be fetched from servers setup on a user's network. Another action category is traps, which are actions that occur when an SNMP trap, an HTTP event, a DMI indication, or similar type of trap or event is received. The trap is turned into an action that is operated on just as any other action. The tools in this category allow the user to forward the trap to other management consoles, to page the user, provide correlation, etc.

In general, management is often classified by what is being managed: hardware, operating system, software, etc. The following Table 1 illustrates the layers and the management data that is typical of that layer. It is noted that Table 1 is by no means exhaustive and simply provides typical management data for the corresponding layer. (emphasis added)

Thus, this section states that the management server handles action categories. One of the action categories is a threshold action category. The user configures situations for the management server to monitor. When certain conditions arise, the user is automatically notified by the system. Thus, an administrator is not sending a notification to the user. Rather, it is the management server that is automatically sending the notification to the user. Another action category is software updates. When a new software update is available, the management server automatically notifies the user that a new software update is available. Once again, there is no administrator involved in sending any type of notification to the user.

While this section of Stupek teaches the feature of allowing a user to monitor management data and then receive notification when certain conditions arise, there is absolutely nothing in this section or any other section of Stupek that teaches or suggests an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. This is because Stupek is not concerned with sending particular alarm messages to a list of users based on profile information.

Stupek is concerned with accessing a network management server and managed devices remotely from a client system via an intranet or the Internet using a web browser. The user can specify certain criteria for the operation of the management server such as which events to monitor. There is nothing in Stupek that even alludes to an administrator sending alarm messages to a list of users, selected from a plurality of users within a profile table. As set forth

above, all notifications to the user are sent automatically from the management server, not from an administrator. In other words, the users do not send notifications to themselves.

Thus, in view of the above, Appellant submits that Stupek does not teach or suggest each and every feature of independent claims 1, 8, and 15 as required under 35 U.S.C. § 103(a). At least by virtue of their dependency on claims 1, 8, and 15, Stupek does not teach or suggest each and every feature of dependent claims 2-7, 9-14, and 16-24. Accordingly, Appellant respectfully requests withdrawal of the rejection of claims 1-21 under 35 U.S.C. § 103(a).

IV. 35 U.S.C. § 103, Alleged Obviousness of claims 2-5, 7, 9-12, 14, 16-19, and 21

The Final Office Action rejects claims 2-5, 7, 9-12, 14, 16-19, and 21 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) in view of Drala software, "Event Notifier, a Pattern for Event Notification," published in Java Report, July 1998, Volume 3, Number 7 (referred to as "Drala" herein).

This rejection is respectfully traversed for at least the same reasons as noted above with respect to claims 1, 8, and 15 from which claims 2-5, 7, 9-12, 14, 16-19, and 21 depend. Specifically, Stupek does not teach or suggest an administrator associated with a server sending alarm messages to a list of users selected from a plurality of users within a profile table. In addition, Drala does not provide for these deficiencies of Stupek.

Drala is directed towards a method for event notification in a network management system. Drala is concerned with the difficulty in adding managed objects to a network. In a simplistic approach, a managed object must send notification of problems to both a console and a paging system. In order to change the interface to the console or the paging system, or add an electronic mail system, every managed object must be modified. Thus, Drala teaches a method for minimizing the number of dependencies and interconnections between objects to prevent the system from becoming difficult to modify. Therefore, Drala is not concerned with directing messages to a set of users on a network. Drala merely teaches an event management scheme that simplifies modifying components within the network management system by making more independent the managed objects from each other and from the console and paging system.

Thus, Drala also does not teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table

as recited in claims 1, 8, and 15 of the present invention (Drala, Motivation section, pages 2-3). Therefore, since neither Stupek nor Drala teach or suggest the features recited in claims 1, 8 and 15, any alleged combination of Stupek and Drala still would not result in these features being taught or suggested. As a result, dependent claims 2-5, 7, 9-12, 14, 16-19, and 21 are allowable over the alleged combination of Stupek and Drala at least by virtue of their dependency on claims 1, 8 and 15, respectively.

In addition to the above, neither Stupek nor Drala, either alone or in combination teach or suggest all of the specific features recited in dependent claims 2-5, 7, 9-12, 14, 16-19, and 21. For example, with regard to claims 4, 11, and 18, neither Stupek nor Drala, alone or in combination teaches or suggests an alarm message is automatically sent at the occurrence of a condition or event. As noted above with regard to claims 1, 8, and 15, Stupek teaches a method for accessing information via the Internet by logging into the network management system and requesting information from the management system. Nowhere does Stupek even allude to a message being sent from a server automatically, in other words, without a request from the administrator. The user of the Stupek system is required to request the information that is to be viewed at the client. Further, with regard to the discussion above, Drala is not concerned at all with the transmission of alarm messages to a list of users. Rather, Drala is focused on a more amenable system for modifying and changing components.

Furthermore, Appellant agrees with the Examiner that neither Stupek nor Drala teaches or suggests the alarm messages are previously written by the administrator as also recited in claims 4, 11, and 18. Rather than actually finding this feature in any secondary reference, however, the Examiner merely alleges that this feature is old and well known. Appellant respectfully disagrees and requests that the Examiner cite a reference in support of the allegation that alarm messages, previously written by an administrator are automatically sent to a set of users based on profile information at the occurrence of a condition or an event. Furthermore, neither Stupek nor Drala is concerned with sending alarm messages to a list of users, selected from a plurality of users within a profile table, regardless of whether the messages were previously written. Thus, neither Stupek nor Drala even suggests alarm messages, previously written by the administrator are automatically sent at the occurrence of a condition or an event as recited in claims 4, 11, and 18 of the present invention.

Additionally, with regard to claim 5, 12, and 19, neither Stupek nor Drala, alone or in combination teaches or suggests that alarm messages are automatically sent when any specific resource monitored by an SNMP via an SNMP interface comes down or becomes unavailable. As with the discussion above, Stupek teaches a method for accessing information via the Internet by logging into the network management system and requesting information from the management system. Stupek does not teach or suggest anywhere that a message is sent from a server automatically when any specific resource monitored by an SNMP via an SNMP interface comes down or becomes unavailable. The user of the Stupek system is required to request the information that is to be viewed at the client. Further, with regard to the discussion above, Drala is not concerned at all with the transmission of alarm messages to a list of users. Rather, Drala is focused on a system that is more amenable to modification.

In rejecting claims 5, 12 and 19, the Final Office Action alleges that the features of these claims are taught by Stupek in column 5, lines 5-67. While this section of Stupek mentions SNMP at lines 28-32 and again at lines 60-63, there is nothing in this section regarding sending alarm messages automatically when any specific resource monitored by a SNMP via a SNMP interface comes down or becomes unavailable. To the contrary, these sections of Stupek merely mention SNMP converter 122 that converts SNMP based data from SNMP managed devices to HTML and that the management server 102 periodically collects and saves configuration information in a common form regardless of whether it was in an SNMP form. Merely mentioning SNMP does not render obvious the specific features in claims 5, 12 and 19 and thus, the Final Office Action has not established a prima facie case of obviousness with regard to the features in these claims.

Furthermore, with regard to claims 3, 10, and 17, Appellant agrees with the Examiner that neither Stupek nor Drala teaches or suggests that alarm messages are written and manually sent by the administrator when necessary. The Examiner alleges that a user can compose a short message and manually send that message as in a conventional e-mail system. While this may be true, the present invention does not claim an e-mail system. The present invention actually claims that alarm messages are written and manually sent by an administrator, to a list of users selected from a profile table that stores profiles of each of the users in a plurality of users, when necessary. In other words, an administrator sends an alarm message in response to a condition or an event that necessitates an alarm message. Neither Stupek nor Drala even suggest such a

feature. This is, in part, because neither Stupek nor Drala teach or suggest communication of any kind between the administrator and a list of users. To the contrary, both Stupek and Drala are directed to notifying the administrator when an event has occurred. Neither reference has anything to do with sending alarm messages to a list of users selected from a profile table that stores profiles for a plurality of users.

Thus, in addition to their dependency on claims 1, 8 and 15, claims 3-5, 10-12 and 17-19 are also allowable over the alleged combination of Stupek and Drala by virtue of the specific features recited in these claims.

V. 35 U.S.C. § 103, Alleged Obviousness of claims 6, 13, and 20

The Office Action rejects claims 6, 13, and 20 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Stupek, Jr. et al. (U.S. Patent No. 6,131,118) in view of Drala software, "Event Notifier, a Pattern for Event Notification," published in "Java Report," July 1998, Volume 3, Number 7, and further in view of Cote et al. (U.S. Patent No. 6,021,262). This rejection is respectfully traversed for at least the same reasons as noted above with regard to claims 1, 8, and 15 from which claims 6, 13, and 20 depend, respectively.

As noted above with regard to claims 1, 8, and 15, neither Stupek nor Drala, either alone or in combination, teach or suggest an administrator associated with a server sending alarm messages to a list of users selected from a plurality of users within a profile table. In addition, Cote does not provide for the deficiencies of the proposed Stupek-Drala combination.

Cote is directed to a system for automatically monitoring the status of messaging software. If a deficiency, such as a software condition or a link condition, is detected in the messaging software, the administrator is notified regardless of whether the message system is non functional. At the point of notification, the deficiency can be resolved by, for example, restarting the server which controls the messaging service (column 1, line 66 – column 2, line 57).

As with Stupek and Drala, Cote does not teach or suggest an administrator sending alert messages to a list of users selected from a plurality of users in a profile table that stores profiles of each of the users. Cote merely teaches sending messages to an administrator when there is a problem with a messaging system. Thus, any alleged combination of Stupek, Drala and Cote still

would not result in the invention as recited in independent claims 1, 8 and 15 from which claims 6, 13 and 20 depend.

Furthermore, there is no teaching or suggestion in either of Stupek or Drala regarding the need or desirability of including a schedule of settings as taught by Cote or how such a schedule of settings would be incorporated into the systems of Stupek and Drala assuming that one of ordinary skill in the art would be somehow motivated to make such a combination. That is, taking the three references alone, i.e. without a prior knowledge of Appellant's claimed invention, one of ordinary skill in the art would not see anything in the actual teachings of the references that would suggest the desirability to combine them or modify them in the particular way that would be necessary to arrive at the claimed invention. Thus, the only way in which one of ordinary skill in the art would be motivated to combine the references and modify them is if that person had a prior knowledge of the claimed invention and the sole purpose of trying to recreate the claimed invention from the parts described in the Stupek, Drala and Cote references. This is clearly hindsight reconstruction using Appellant's own disclosure as a guide and is an improper basis upon which to make a rejection under 35 U.S.C. § 103(a).

Examiner's Response to Appellant's Arguments

In response to Appellant's argument that the Examiner is engaged in hindsight reconstruction with the proposed combination of references, the Examiner, in the Final Office Action, merely uses the form paragraph response that "any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning but so long as it...does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper." Appellant respectfully submits that in the present case, the Examiner has taken knowledge gleaned only from Appellant's disclosure and used it to manufacture the rejection based on Stupek, Drala and Cote and the Examiner has not shown by his response that this is not the case. Nowhere in any of the references is there any teaching of selecting users from a plurality of user profiles in a profile table and an administrator sending alert messages to the selected users. To the contrary, as shown above, the references are directed to notifying an administrator of events occurring in a system. Thus, the only way in which the references could be combined and modified to arrive at the claimed invention is to first have benefit of the claimed invention and then the sole purpose

of using the bits and pieces taken from the available references, modify them to work in a different manner, and then combine them to arrive at the claimed invention. This is clearly hindsight even taking the Examiner's statement that "any judgement of obviousness is in a sense necessarily a reconstruction..." into account. Thus, the Examiner has failed to illustrate why the alleged combination should not be considered an impermissible hindsight reconstruction of Appellant's claimed invention.

VI. Unclear Status of Rejections of Claims 22-24

The first Office Action rejects independent claims 1, 8 and 15 under 35 U.S.C. § 103(a) based on Stupek, Jr. et al. (U.S. Patent No. 6,131,118). The Final Office Action then rejects newly added claims 22-24 under 35 U.S.C. § 102(e) based on Raffel et al. (U.S. Patent Publication 2002/0082892) and Ruckdashel et al. (U.S. Patent No. 6,038,542). However, claims 22-24 are dependent claims that are dependent from independent claims 1, 8 and 15, respectively. Thus, according to the Final Office Action, the independent claim is rejected under 103(a) based on Stupek, yet the dependent claims are rejected under 102(e) based on either of Raffel or Ruckdashel. Thus, it is unclear as to whether claims 22-24 are intended to be rejected under 35 U.S.C. § 102(e) as stated or under 103(a) based on a combination of Stupek and either Raffel or Ruckdashel.

Moreover, it is unclear as to whether claims 1, 8 and 15 are rejected under 102(e) based on Raffel and Ruckdashel. Under the current statement of the rejections, it is possible that Appellant may overcome the rejection of claims 22-24 based on Raffel and Ruckdashel and the application may issue as a patent and yet the question of whether independent claims 1, 8 and 15 are allowable over Raffel and Ruckdashel may still be unanswered. The Examiner is required to set forth the best art and all appropriate rejections and thus, if the Examiner believes that claims 22-24 are anticipated by Raffel and Ruckdashel, then the Examiner must also set forth a rejection of their independent claims 1, 8 and 15 based on alleged anticipation.

Thus, in addition to the other reasons set forth herein, the Final Office Action should be overturned and a new Office Action issued that clearly states the basis for the rejections of each of the claims setting forth the best art and appropriate rejections. For purposes of the present Appeal, however, the application of Raffel and Ruckdashel to the actual features of independent

claims 1, 8 and 15 will be addressed in the arguments regarding claims 22-24 to thereby illustrate why a rejection under 35 U.S.C. § 102 of claims 1, 8 and 15 based on this art would be improper if made.

VII. 35 U.S.C. § 102, Alleged Anticipation of Claims 22-24

The Final Office Action rejects claims 22-24 under 35 U.S.C. § 102(e) as being allegedly anticipated by Raffel et al. (U.S. Publication No. 20020082892). This rejection is respectfully traversed.

As with Stupek, Raffel does not teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. Therefore, whether the rejection is based solely on Raffel as stated, or on an alleged combination of Raffel and Stupek, the features of claims 22-24 are not taught or suggested by the references.

Raffel is directed to a system for providing transactional information of deals, contracts, accounts and leads over the internet. The transactional information is accessed and shared among members of the host organization. The transactional information can be imported into other applications such as, for example, a spreadsheet. An administrator is responsible for providing each authorized user with materials necessary to use the system such as software and access information. In addition, the administrator can configure the system to notify users every time there is new or changed information for accounts or deals to which a user has access.

Thus, Raffel is concerned, in part, with notifying users when information in the system corresponding to accounts or deals is updated. While Raffel may teach sending a notification to a user, there is nothing in Raffel that teaches that an administrator associated with a server sends an alarm message to a list of users, selected from a plurality of users, within a profile table. To the contrary, the administrator in Raffel configures the system to automatically send out notifications as stated in paragraph 0082 of Raffel, which reads as follows:

> The territorial configuration of the CIMS system provides a way to create groups of related accounts, contacts, and deals and to designate groups of users who have a responsibility to manage and track business taking place within each territory. In one embodiment, system administrators have the ability to establish and maintain territory definitions and to determine access rights of users to the

territories, but the embodiment is not so limited. Territories are important in that they limit access to potentially sensitive deal information. By setting up territories so that they reflect the way an organization does business and by assigning appropriate staff members to each territory, only those users who are authorized to do so will be able to view or change confidential information relating to a territory. Furthermore, territories can be used to aggregate accounts and deals for reporting, filtering, and notification. For example, users may create profiles that show accounts, contacts, or deals in specific territories. Moreover, a system administrator may configure the CIMS to notify users every time there is new or changed information for accounts or deals that are located only in their territories. This enables the member of a particular sales team to focus on the information that is most critical to them. (emphasis added)

Thus, once the administrator selects which events will trigger a notification, the system automatically sends the notifications to the users. Claims 1, 8 and 15 of the present invention recite that the administrator sends the alarm to a list of users, selected from the plurality of users within the profile table. This is a manual process performed by an administrator and not an automatic process such as that taught in Raffel. Therefore, the rejection of claims 22-24 under 35 U.S.C. § 102(e) is overcome.

VIII. 35 U.S.C. § 102, Alleged Anticipation of Claims 22-24

The Final Office Action rejects claims 22-24 under 35 U.S.C. § 102(e) as being allegedly anticipated by Ruckdashel et al. (U.S. Patent Mo. 6,038,542). This rejection is respectfully traversed.

As with Stupek, Ruckdashel does not teach or suggest an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users within a profile table. Therefore, whether the rejection is based solely on Ruckdashel as stated, or on an alleged combination of Ruckdashel and Stupek, the features of claims 22-24 are not taught or suggested by the references.

Ruckdashel is directed to a system for notifying an individual of a scheduled event. A server retrieves a user's schedule information and analyzes the information. Events within a specified time frame are queued and a notification server is activated at the time that the queued event is to occur. The user is then notified of the event.

As in Raffel, the process of notifying the user is automated. The administrator's main

task in Ruckdashel is to maintain the database of users by adding and deleting users. The actual notification is performed by notification software. Thus, Ruckdashel does not teach an administrator associated with a server sending alarm messages to a list of users, selected from a plurality of users, within a profile table. Therefore, the rejection of claims 22-24 under 35 U.S.C. § 102(e) is overcome.

CONCLUSION

For the reasons set forth above, Appellant respectfully submits that claims 1-24 are in condition for allowance over the cited art of record. Accordingly, Appellant respectfully requests that the Board of Patent Appeals and Interferences overturn the rejections and objections set forth in Final Office Action.

Respectfully submitted,

Stephen J. Walder, Jr.
Reg. No. 41,534
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The text of the claims involved in the appeal are:

1. System for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using Java language, said system being characterized in that it comprises:

a profile table containing profiles of each one of said plurality of users; and

processing and transmitting means enabling an administrator associated with said server to transmit alarm messages to the list of users wherein said users have been selected from said profile table, said alarm messages being displayed on a screen of a workstation associated with each selected user if said workstation is running.

2. The system according to Claim 1, wherein said processing and transmitting means comprise a processing unit operating under the control of a Java alarm program and a message sender transmitting directly said alarm messages over said network.

3. The system according to Claim 2, wherein said alarm messages are written and manually sent by the administrator when necessary.

4. The system according to Claim 2, wherein said alarm messages previously written by the administrator are automatically sent by said processing and transmitting means at the occurrence of a condition or an event.

5. The system according to Claim 4, wherein said alarm messages are automatically sent when any specific resource monitored by a Simple Network Management Protocol (SNMP) via a SNMP interface comes down or becomes unavailable.

6. The system according to Claim 4, wherein said alarm messages are automatically sent at the occurrence of an event scheduled in an alarm scheduler by said administrator.

7. The system according to Claim 2, wherein said alarm messages are standalone alarm functions used to detect when said server is out of work.

8. A method of broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet protocol (IP) and using Java, comprising the steps of:

profiling in a profile table each one of said plurality of users;

processing an alarm message by an administrator associated with the server; and

transmitting said alarm message to the list of users wherein said users have been selected from said profile table, said alarm message being displayed on a screen of a workstation associated with each selected user if said workstation is on.

9. The method according to Claim 8, wherein said steps of processing and transmitting comprise operating a processing unit under the control of a Java alarm program and a message sender transmitting directly said alarm messages over said network.

10. The method according to Claim 9, wherein said alarm messages are written and manually sent by the administrator when necessary.

11. The method according to Claim 9, wherein alarm messages previously written by the administrator are automatically sent at the occurrence of a condition or an event.

12. The method according to Claim 11, wherein said alarm messages are automatically sent when any specific resource monitored by a Simple Network Management Protocol (SNMP) via a SNMP interface comes down or is unavailable.

13. The method according to Claim 11, wherein said alarm messages are automatically sent at the occurrence of an event scheduled in an alarm scheduler by said administrator.

14. The method according to Claim 9, wherein said alarm messages are standalone alarm functions used to detect when said server is out of work.

15. A computer program product recorded on computer readable medium for broadcasting alarm messages from a server to a list of users among a plurality of multi-platform users sharing the server in a data transmission network operating under Internet Protocol (IP) and using Java language, comprising:

computer readable means for creating a profile table containing profiles of each one of said plurality of users; and

computer readable means for processing and for transmitting to enable an administrator

associated with said server to transmit alarm messages to the list of users wherein said users have been selected from said profile table, said alarm messages being displayed on a screen of a workstation with each selected user if said workstation is running.

16. The program product according to Claim 15, wherein said computer readable means for processing and for transmitting comprise a processing unit operating under the control of a Java alarm program and a message sender transmitting directly said alarm messages over said network.

17. The program product according to Claim 16, wherein said alarm messages are written and manually sent by the administrator when necessary.

18. The program product according to Claim 16, wherein said alarm messages previously written by the administrator are automatically sent by said computer readable means for processing and for transmitting at the occurrence of a condition or an event.

19. The program product according to Claim 18, wherein said alarm messages are automatically sent when any specific resource monitored by a Simple Network Management Protocol (SNMP) via a SNMP interface comes down or becomes unavailable.

20. The program product according to Claim 18, wherein said alarm messages are automatically sent at the occurrence of an event scheduled in an alarm scheduler by said administrator.

21. The program product according to Claim 15, wherein said alarm messages are standalone alarm functions used to detect when said server is out of work.

22. The system according to Claim 1, said system being characterized in that it further comprises:

selection means for selecting, in response to a condition or an event, a list of users based on profile information in the profile table wherein the list of users is a subset of the plurality of users.

23. The method according to Claim 8, further comprising the steps of:

selecting, in response to a condition or an event, a list of users based on profile information in the profile table wherein the list of users is a subset of the plurality of users.

24. The program product according to Claim 15, further comprising:

computer readable means for selecting, in response to a condition or an event, a list of users based on profile information in the profile table wherein the list of users is a subset of the plurality of users.